National Security Agency

INFORMATION
ASSURANCE
DIRECTORATE

Statement by

Michael G. Fleming

Chief, Information Assurance Solutions

Information Assurance Directorate

National Security Agency

Before The

House Committee on

Government Reform

Subcommittee on

Technology, Information Policy, Intergovernmental Relations

and Census

Hearing on

"Exploring Common Criteria: Can it Ensure that the Federal Government Gets Needed Security in Software"

September 17, 2003

For Official Use Only
Until Released by the
U.S. House of Representatives
Committee on Government Reform

Thank you Chairman Putnam and the members of the Subcommittee. I am honored to have the opportunity to speak with your committee to discuss the Common Criteria and the National Information Assurance Partnership (NIAP).

I also would like to thank the Chairman and other members of the Subcommittee for their strong interest and attention to the vital area of cybersecurity. Your leadership is important for raising awareness of the serious security challenges we all face in our age of interconnected, inter-dependent digital networks.

My name is Michael Fleming and I am the Chief of the Information Assurance Solutions Group, Information Assurance Directorate, National Security Agency (NSA). My Group is responsible for developing information assurance solutions, support for the *International Common Criteria for Information Technology Evaluation* (known as the Common Criteria), and the NIAP.

I would like to note that the NSA's Information Assurance Directorate and its predecessor organizations have had technical and policymaking responsibility regarding the protection of national security telecommunications and information processing systems across the Executive Branch since 1953.

In regards to your theme for this hearing: "Exploring Common Criteria: Can it Ensure that the Federal Government Gets Needed Security in Software?" while in the security business it is hard to "ensure" absolutely, we believe the Common Criteria is a very important step in improving the "goodness" of an information assurance (IA) or information assurance enabled (IA-enabled) information technology (IT) product. I would like to provide you with an overview of the Common Criteria and the National Information Assurance Partnership (NIAP) and how it operates, highlight its benefits, and finally discuss the remaining issues associated with the activity. In Appendix A of my statement, you will find a synopsis of the lineage behind both the evolution of the criteria and the evolution of the evaluation programs for commercially produced IA or IA-enabled products to help understand the rationale behind the adoption of the *International*

Common Criteria for Information Technology Security Evaluation (subsequently referred to as the Common Criteria) and the establishment of the (NIAP).

The Common Criteria represents the outcome of an international effort (United Kingdom, France, Germany, Netherlands, Canada, and the United States) to develop criteria for the evaluation of information technology security by providing a standard language or syntax for describing the security requirements of an IA or IA-enabled product or system. Version 1.0 of the Common Criteria was published for comment in 1996, which was extensively reviewed and trialed by several nations. Based upon this review and lessons learned, the Common Criteria Version 2.0 was officially published in May 1998 and adopted by the International Organization for Standard (ISO) as an International Standard (ISO 15408) in August 1999.

For the purposes of this testimony and to put information technology products into perspective, I would like to categorize three types of information technology products; IA, IA-enabled, and other relevant IT products as shown in Figure 1: IA Relevant Technology Spectrum.

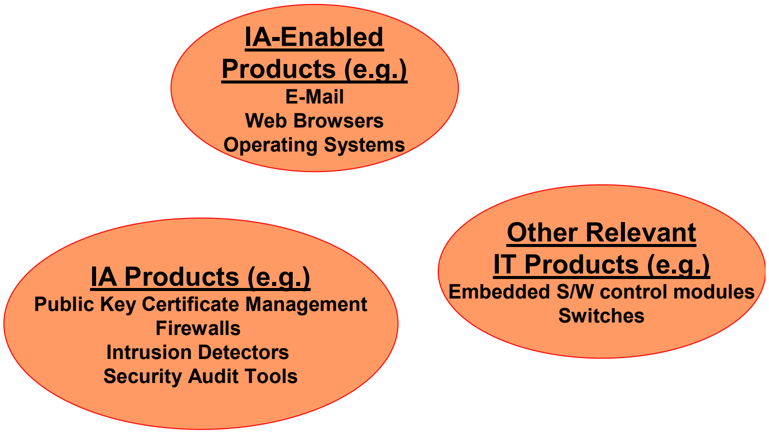
IA-Enabled Products (e.g.)
E-Mail
Web Browsers
Operating Systems
IA Products (e.g.)
Public Key Certificate Management
Firewalls
Intrusion Detectors
Security Audit Tools
Other Relevant IT Products (e.g.)
Embedded S/W control modules
Switches

Figure 1: IA Relevant Technology Spectrum

An IA product's primary purpose is to provide security functionality (e.g., confidentiality, authentication, integrity, access control, or non-repudiation of data).

Examples of an IA product include Public Key certificate management, firewalls, intrusion detection devices, etc. An IA-enabled product is an information technology product whose primary role is not security, but which provides security functionality as an associated feature of its intended operating capabilities. Examples of an IA-enabled product include operating systems and database management systems with IA enabling functions (e.g., identification and authentication, passwords, audit, access controls, etc.), web browsers, e-mail, etc. Other relevant information technology products are those that provide no security functionality but do provide information processing services. Examples of other relevant IT products include switches, embedded software control modules, etc. This category is relevant because these products, while claiming no IA functionality, can be the source of vulnerabilities. An example would be the embedded timing module of a coolant system within a power plant.

One of the major benefits of the Common Criteria is that it establishes a common language for describing consumer security needs and IA or IA-enabled product vendor claims as well as the methodology for independently evaluating how well the claims meet the needs. While the Common Criteria is a very good specification and assessment tool for the security functionality within IA-enabled products, it should be noted that typically this functionality is only a subset of the total functionality of a product. As shown in Figure 2: Common Criteria Application to IA Relevant Technology Spectrum, the Common Criteria is applied to security functionality found in IA and IA-enabled products but is not applied to the functionality of other relevant information technology products since they make no IA claims. A Common Criteria evaluation typically analyzes the security functionality. Any vulnerability that is within an IA-enabled product that may be introduced by non-security functionality could go undetected (i.e., only the claimed IA functionality is typically evaluated).

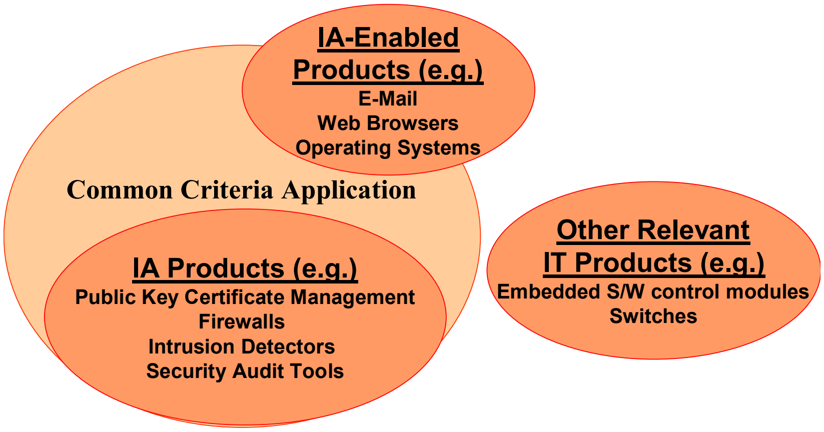
IA-Enabled Products (e.g.)
E-Mail
Web Browsers
Operating Systems
Common Criteria Application
IA Products (e.g.)
Public Key Certificate Management
Firewalls
Intrusion Detectors
Security Audit Tools
Other Relevant IT Products (e.g.)
Embedded S/W control modules
Switches

Figure 2: Common Criteria Application to IA Relevant Technology Spectrum

The Common Criteria employs distinct but related categories of functional requirements and assurance requirements. Functional requirements describe security behavior mechanisms and assurance requirements describe the confidence gaining measures that the claimed security functionality is implemented correctly. For assurance requirements the Common Criteria defines seven (7) evaluated assurance levels (EALs). These EALs are denoted as EAL 1 through EAL 7 with EAL 1 being the lowest and least rigorous evaluation and EAL 7 being the highest and most rigorous evaluation. Further detail regarding the activities that are performed at each of the evaluation assurance levels is found in Appendix C.

International Mutual Recognition

Following the development of the Common Criteria, the authoring nations joined together to develop a Common Criteria Recognition Arrangement (CCRA). This recognition arrangement established the framework for each nation to mutually accept the validity of evaluations conducted by another nation for the first four evaluated assurance levels (EAL 1 through EAL 4) of the Common Criteria. Each member nation agreed that evaluations would be conducted using the Common Criteria and associated Common

Evaluation Methodology (the “how-to” companion document) to provide the member nations confidence that an evaluation would yield the same results regardless of which nation performed the evaluation. Mutual recognition of the product evaluation should not be construed as an endorsement, approval, or recommendation for use of the product by any member nation.

Establishment of the National Information Assurance Partnership

In September 1996, the NIST and the NSA entered into discussions on the creation of a joint testing center to focus on the evaluation of commercially produced IA or IA-enabled products against the emerging Common Criteria. These discussions were the genesis for the current National Information Assurance Partnership (NIAP). On August 22, 1997, the Director of NIST’s Information Technology Laboratory and the Deputy Director of NSA’s Information System’s Security Organization signed the formal Letter of Partnership. The partnership combines the extensive information technology security experience of both organizations to promote the development of technically sound security requirements for IA or IA-enabled products and systems and appropriate measures for evaluating those products and systems. The goal of the NIAP was to increase confidence in IA and IA-enabled products through independent, third party evaluation to help ensure the security of the information technology systems and networks. More specifically, NIAP sought to: 1) promote demand and investment in security products and 2) establish a commercial security product evaluation capability to compliment existing government evaluation and testing efforts. With the background set, lets now take a look at how well the NIAP is meeting its stated goals.

National Information Assurance Partnership Goal Achievement

The NIAP’s first goal was to promote demand and investment in IA and IA-enabled products. One of the major benefits of the Common Criteria is that it establishes a common language to describe consumer security needs and/or IA and IA-enabled product vendor claims, as well as establishes the mechanism for independently evaluating how well the claims meet the needs.

In support of efforts to increase the use and availability of evaluated products the National Security Telecommunications Information Systems Security Committee (NSTISSC), which is now known as the Committee on National Security Systems (CNSS) issued NSTISSC Policy Number 11 (NSTISSP No. 11) in January 2000. The CNSS consists of representatives from 21 U.S. Government Departments and Agencies (listed in Appendix B).

NSTISSP No. 11 stipulates that information assurance (IA) shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated and validated Government Off-the-Shelf (GOTS) or Commercial Off-the-Shelf (COTS) IA and IA-enabled Information Technology (IT) products. As of 1 July 2002, the acquisition of COTS IA and IA-enabled IT shall be limited to those products which have been evaluated and validated in accordance with the following:

1) The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program,
2) The NIST Federal Information Processing Standard (FIPS) Cryptographic Module Validation Program, or
3) The International Common Criteria For Information Security Technology Evaluation Mutual Recognition Arrangement.

The acquisition of all GOTS IA and IA-enabled products shall be limited to those products which have been evaluated by the NSA, or in accordance with NSA-approved processes. The policy further stipulates that normally a complementary combination of IA and IA-enabled products are needed to provide a complete security solution to a given environment.

NSTISSP No. 11 did not stipulate specific security requirements from a functional or assurance point of view. The intent of NSTISSP No. 11 was to allow vendors to make claims about their products that could be validated and for consumers to decide if the validated requirements satisfied their needs. Paragraph 4 of NSTISSP No. 11 says; "it is important that COTS products acquired by U.S. Government Departments and Agencies be subject to a standardized evaluation process which will provide some assurances that these products perform as advertised." By not stating any specific requirements other than evaluation, NSTISSP No. 11 gives vendors the flexibility make evaluatable claims about their product's security functionality at a given assurance level using Common Criteria language that can be independently validated.

One of the major thrusts of the NIAP has been on using the Common Criteria as a way to state the security requirements that are needed by U.S. Government consumers in critical technology areas. The Common Criteria documents that state these security requirements are called Protection Profiles. Protection Profiles define an implementation-independent set of security requirements and objectives for a category of IA and IA-enabled products, which would meet the needs of a particular application environment. A Protection Profile has 6 sections that must be addressed so that it can be evaluated for conformance to the Common Criteria (see Appendix D).

Based on discussions with vendors and users (DoD and other Federal Government agencies), the NSA Information Assurance Directorate and the NIST have identified key IA and IA-enabled technologies and have undertaken efforts to define Protection Profiles for them. These key technologies include Operating Systems, Firewalls, Wireless, Web, Intrusion Detection Systems (IDS), Tokens, Databases, Virtual Private Networks (VPN), Biometrics, and Public Key Infrastructure (PKI). Currently, there are 21 finalized Protection Profiles of which eighteen (18) are U.S. Government and three (3) are from commercial organizations. Additionally, there are thirty-one (31) new U.S Government Protection Profiles under development.

DoD Directive 8500.1, “Information Assurance” and DoD Instruction 8500.2, “Information Assurance (IA) Implementation” characterize security application environments as needing low, medium and high security robustness. As such, the U.S. Government Protection Profiles state the security requirements necessary to protect information within the various security robustness environments.

The combination of these policy based demand incentives have been encouraging. As U.S. Government Protection Profiles are introduced for a particular technology sector, the number of evaluations claiming compliance with a Protection Profile has been increasing. For example 100% of all operating systems evaluations, 100% of all Public Key Infrastructure Certificate Issuing Management Components, 61.5% of all Firewalls, and 60% of all intrusion detection systems are claiming compliance or have met U.S. Government Protection Profiles.

The second goal of the partnership was to establish a commercially based evaluation and testing scheme to compliment existing government evaluation capabilities. The NIAP developed and established the policies and procedures for participation in the Common Criteria Evaluation and Validation Scheme and established the Common Criteria Evaluation and Validation Scheme Validation Body in 2000. This jointly staffed organization approves participation of commercial security testing laboratories in the scheme, provides technical guidance to those testing laboratories, validates the results of IA and IA-enabled product evaluations for conformance to the Common Criteria, and serves as an interface to other nations for the mutual recognition of such evaluations. Since its implementation the Common Criteria Evaluation and Validation Scheme has accredited, through the NIST sponsored National Voluntary Laboratory Accreditation Program (NVLAP), nine (9) commercial evaluation facilities, with eight (8) of these facilities still actively participating in the scheme to date. As of 31 August 2003, these facilities have completed thirty-eight (38) evaluations of IA and IA-enabled products. Additionally, there are currently fifty-five (55) IA and IA-enabled product evaluations currently on-going within the commercial evaluation facilities with these facilities negotiating new evaluation contracts daily. These products, produced by large as well as small corporations, are from the spectrum of IA and IA-enabled products.

In order for the IA or IA-enabled product to be evaluated, the vendor of the product must develop a Common Criteria specification known as a "Security Target." Unlike a Protection Profile, a Security Target is implementation specific. The Security Target contains all of the sections of a Protection Profile with an additional seventh section called the Target of Evaluation (TOE) Summary Specification. This section is where the vendor describes how their product satisfies the security requirements based on the environment, assumptions, policies, threats, and objectives.

Once a Security Target has been created, the IA or IA-enabled product vendor takes the Security Target to a NIAP approved or international mutually recognized Common Criteria Testing Laboratory (CCTL) for formal evaluation. Upon successful completion of the evaluation, a Common Criteria certificate is issued to the IA or IA-enabled product vendor and the Security Target and Validation Report are made available to the public (http://niap.nist.gov/cc-scheme/ValidatedProducts.html).

Aspects and Benefits of Criteria Based Evaluation

Along with the technology explosion comes a desire of the consumer to have confidence when they utilize their IA and IA-enabled products that their exposure to vulnerabilities are keep to a minimum. Even with a criteria based evaluation, no product can be deemed "Bullet-Proof." Vulnerabilities can be introduced in a number of ways from product design and development, through poor implementation of their design, and through operation of the system. Vulnerabilities can be introduced into a product or system at the requirements definition phase if insufficient or ineffective requirements are incorporated into the product design. During the construction of the product, vulnerabilities can arise from incorrect design decisions or errors in design implementation. Once a product/system is installed, vulnerabilities can be introduced due to inadequate controls or enforcement of these controls in the operational environment.

The question is how a criteria based evaluation can aid the consumer in mitigating most of the risks associated with using an IA and IA-enabled product. Being able to specify the needed security features (functionality) and the level of confidence (assurance) for IA and IA-enabled products is an important first step in building more secure systems. Using Protection Profiles provides manufacturers with a potential build to specification and a known potential market. Using an independent evaluation provides the consumer with a level of confidence that the vendor's claims are indeed valid. This confidence is gained through the various activities associated with an evaluation. The combination of activities and the rigor to which they would be applied will increase as the evaluation assurance level increases.

What are some of the Issues with the Common Criteria

The cost and timeliness of a Common Criteria evaluation varies depending on a number of factors: the complexity of the IA or IA-enabled product and the claims made in the Security Target; the Evaluated Assurance Level chosen (the higher the EAL the more likely the higher the costs); the vendor's preparedness to undergo an evaluation (vendors must provide specific documented evidence to support their claims); and problems found in conforming to the requirements must be fixed before the IA and IA-enabled product can complete evaluation. These costs are usually passed on to the consumer making evaluated IA and IA-enabled products more expensive than non-evaluated IA and IA-enabled products. However, the criteria and the NIAP evaluation program are structured such that a vendor can capitalize on their initial evaluation investment and re-utilize most if not all of their previous evaluation work to significantly reduce the cost and timeframe for subsequent evaluations of their next release at the same Evaluated Assurance Level or to migrate the evaluated product to a higher Evaluated Assurance Level.

While a criteria based evaluation makes every attempt to identify and correct security vulnerabilities and/or flaws within an IA and IA-enabled product from a security perspective given the size and complexity of most products and large number of lines of code, it cannot ensure that the product is “Bullet-Proof”, especially at the lower Evaluated Assurance Levels. The security functionality within an IA-enabled product is only a subset of all the functionality within the product. A Common Criteria evaluation will only analyze the security functionality at the selected Evaluated Assurance Level. Access to and evaluation of full source code is not required until the Evaluated Assurance Level 5, which is generally higher than most commercial vendors aspire to. Vulnerabilities within an IA-enabled product that are introduced by non-security functionality may go undetected. Historically, these vulnerabilities have been the most exploited. A significant cyber security challenge will be found in enhancing our ability to find and eliminate malicious code in large software applications. Beyond the matter of simply eliminating coding errors, this capability must find malicious software routines that are designed to morph and burrow into critical applications in an attempt to hide.

Applicability of Common Criteria Across Government and Beyond

The requirements for Information Protection and Information Assurance in our traditional national security market are almost identical to the IA requirements found in mission-critical government systems and the commercial critical information protection market. Many of these systems will be coming under the direct control or influence of the Department of Homeland Security. Legislation as recent as the Healthcare Information Protection and Privacy Act recognizes the need to protect and individual’s information.

We must accelerate the convergence of these markets and use the emerging Homeland Security policies to join these three communities into a single unified market for IA products. The unification on the demand side of the IA market will naturally result in greater interest on the supply side of the market to develop compliant systems. A larger market results in greater return on investment (ROI) for vendors, and everyone in the IA market benefits from the resulting reduced costs, increased functionality, and greater assurance. A “converged market” for IA products market will also significantly increase the potential for interoperability among national security, mission-critical government, and critical infrastructure protection systems, to include similar systems operated by our international trading partners and military allies. The U.S. Government cannot afford to develop and deploy IA systems that do not interoperate or that require complex configuration or costly system management structures.

The Common Criteria and the NIAP evaluation scheme offer a mechanism for providing a standardized specification of these IA needs and an independent third party evaluation of a product’s conformance to these needs. Through the use of the NIAP evaluation program coupled with widely accepted Protection Profiles by the government and industry, a "converged market" could be created.

Conclusion

All information systems require the element of assurance. Assurance that the system was specified and designed properly. Assurance that it was independently evaluated against a prescribed set of explicit security standards. Assurance it will maintain proper operation during its lifetime, even in the face of malicious attacks and human error.

The Common Criteria and NIAP are working, the trends are up and process improvements continue.

A converged market for security products would benefit all buying sectors and the IA and IA-enabled product vendors.

The Common Criteria and NIAP are not a panacea for all security issues for all information technology. We need complementary activities. It has been my experience that security is most effective when it is “baked in” to information systems starting with specification and continuing through design and development. Assurance cannot be "evaluated in" or sprinkled over a system after it is fielded.

It has been my pleasure to discuss the Common Criteria and to share the work of the NIAP with the sub-committee today and I thank you for the opportunity.

Appendix A

Evolution of Evaluation Criteria

A Defense Science Board Task Force report, “Security Controls for Computer Systems,” published in February 1970, made a number of policy and technical recommendations on actions to be taken to reduce the threat of compromise of classified information processed on remote-access computer systems. Department of Defense Directive 5200.28 and its accompanying manual DoD 5200.28-M, published in 1972 and 1973 respectively, responded to one of these recommendations by establishing uniform DoD policy, security requirements, administrative controls, and technical measures to protect classified information processed by DoD computer systems.

Concurrent with DoD efforts to address computer security issues, work was begun under the leadership of the National Bureau of Standards (NBS) (the predecessor to the National Institute of Standards and Technology (NIST)) to define problems and solutions for building, evaluating, and auditing secure computer systems. As an outgrowth of recommendations from this work, and in support of the DoD computer security initiative, the MITRE Corporation began work on defining computer security evaluation criteria that could be used to assess the degree of trust one could place in a computer system to protect classified data.

The National Bureau of Standards and MITRE evaluation material evolved into the *Department of Defense Trusted Computer Systems Evaluation Criteria* (also known as the Orange Book or DoD 5200.28-STD) which was released in 1983. It was later updated and re-released in December 1985 and served as the evaluation criteria for systems used within the federal government from 1985 until 2000.

In the late 1980’s Canada developed a similar criteria known as the *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC) and the European Community developed the *Information Technology Security Evaluation Criteria* (ITSEC). Each established an accompanying evaluation program for commercial IA or IA-enabled product evaluation against the respective criteria.

In 1990, the NIST and the NSA launched an initiative to update the *DoD Trusted Computer Systems Evaluation Criteria* with a new jointly developed criteria for all of federal government known as the *Federal Criteria*. The Canadian and the European Community were also launching initiatives at this time to update their respective criteria. However in 1993, prior to the completion of the Federal Criteria, an international coalition of nations which included the United Kingdom, France, Germany, Netherlands, Canada, and the United States (NSA and NIST) reached agreement that a common security evaluation criteria should be developed rather than having a separate security evaluation criteria for each nation. The vendors of IA and IA-enabled products favored this approach because it would eliminate the need for three unique evaluations of the same product. This led to a pooling of international experts and resources directed towards the production of the *International Common Criteria for Information Technology Security Evaluation*. Version 1.0 of the Common Criteria was published for comment in 1996, which was extensively reviewed and trialed by several nations. Based upon this review and lessons learned, the Common Criteria Version 2.0 was officially published in May 1998 and adopted by the International Organization for Standard (ISO) as an International Standard (ISO 15408) in August 1999.

Evolution of Evaluation Programs

The National Computer Security Center, formerly named the DoD Computer Security Evaluation Center, was formed in January 1981 to staff and expand on the work started by the DoD computer security initiative.

The NSA through the National Computer Security Center implemented the Trusted Product Evaluation Program for the evaluation of commercially available computer systems against the *DoD Trusted Computer Systems Evaluation Criteria*. The Trusted Product Evaluation Program utilized government evaluators from the NSA and selected Federally Funded Research and Development Centers.

In December 1994, the NSA based on a NIST proposal and with their cooperation, took actions to implement a commercially based IA or IA-enabled product evaluation program. During this time of information technology explosion, IA and IA-enabled product explosion, and government downsizing, evaluation responsibilities shifted from a government funded and staffed evaluation program to a commercially-based, fee for service evaluation program. This action was essential if the U.S. was to maintain a viable program for the assessment of commercial-off-the-shelf (COTS) IA and IA-enabled products in a timely and cost effective manner. The decision for this fundamental shift was predicated upon the resource limitations of the government coupled with the lengthy timeframe for acceptance into and completion of an evaluation. After a two (2) year development and training effort, the NSA implemented the Trust Technology Assessment Program in January 1997, approving six commercial evaluation facilities to conduct evaluations against the *DoD Trusted Computer Systems Evaluation Criteria* with the IA or IA-enabled product vendor funding the cost of the commercial evaluation. The NSA continued to maintain oversight of each evaluation and issued the certificate of completion and compliance to the criteria.

Appendix B

Members of the Committee on National Security Systems (CNSS)

Department of State

Department of Treasury

Department of Defense,

Department of Justice

Department of Commerce

Department of Transportation

Department of Energy

Office of Management and Budget

Central Intelligence Agency

Federal Bureau of Investigation

Federal Emergency Management Agency

General Services Administration

US Army

US Air Force

US Navy

US Marine Corp

National Security Agency

National Communication System

Defense Intelligence Agency

The Joint Chiefs of Staff

Assistant to the President for National Security Affairs

Permanent observers represent the Defense Information Systems Agency (DISA), Department of Education, Federal Communications Commission (FCC), National Aeronautics and Space Administration (NASA), National Imagery and Mapping Agency (NIMA), National Institute of Standards and Technology (NIST), Nuclear Regulatory Commission (NRC), Chairman, Subcommittee on Information Systems Security (SISS), Security Policy Board Staff (SPB), National Reconnaissance Office (NRO), and the Critical Infrastructure Assurance Office (CIAO).

Appendix C

Evaluated Assurance Levels

The activities used to gain assurance about an IA and IA-enabled product and the rigor to which they are applied increases as you move up the Evaluated Assurance Levels from 1 to 7. These activities include an analysis of the process and procedures used in the development of the product with a corresponding check to ensure that the process and procedures are/were being applied to the development of the product. An analysis of the requirements can be conducted to ensure they are sufficient and effective for the product's functionality and security purposes. These requirements can be further traced to the design representations to ensure they are reflected in the product design. The product can be analyzed to ensure that the actual product is reflective of the design representations thus insuring that all requirements have been implemented. Additionally, one can perform an analysis of the vendor's functional tests and test results to ensure that the product was adequately tested and yielded appropriate test results. The evaluation team could also perform their own independent functional testing as well as conduct penetration testing to see if they can break into the product or by-pass security mechanisms within the product. A flaw analysis of the product can be conducted in an attempt to insure that IA and IA-enabling feature flaws can be kept to a minimum. And lastly, an analysis of guidance documentation provided by the vendor can be conducted to insure that it adequately describes the IA attributes of the product and processes and procedures for appropriately utilizing them.

Various of these activities are applied to meet the following Common Criteria defined evaluated assurance levels.

EAL 1 – Functionally tested

EAL 2 – Structurally tested

EAL 3 – Methodically tested and checked

EAL 4 – Methodically designed, tested and reviewed

EAL 5 – Semiformally designed and tested

EAL 6 – Semiformally verified design and tested

EAL 7 – Formally verified design and tested

Appendix D

Protection Profile Sections

A Protection Profile has 6 sections that must be addressed so that it can be evaluated for conformance to the Common Criteria. These sections are:

1) Security Environment – in this section the consumer describes the environment in which they would see this IA or IA-enabled product being used.
2) Secure Usage Assumptions – the consumer describes assumptions made about the IA or IA-enabled product in the areas of connectivity, physical locations, and personnel.
3) Organizational Security Policies - this section describes any organization security policies that the IA or IA-enabled product would be expected to enforce.
4) Threats to Security – the consumer identifies the threats that the IA or IA-enabled product is expected to address and the threats that the operating environment is expected to address.
5) Security Objectives - this section identifies the security objectives that should be achieved through the use of this IA or IA-enabled product.
6) Security Requirements – the consumer selects from Part 2 of the Common Criteria the functional requirements and from Part 3 of the Common Criteria the assurance requirements for which they would like to have an IA or IA-enabled product validated against.